

**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ****(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ**(21), (22) Заявка: **2006115366/09, 06.10.2004**(24) Дата начала отсчета срока действия патента:
06.10.2004(30) Конвенционный приоритет:
09.10.2003 US 10/605,574(43) Дата публикации заявки: **20.11.2007**(45) Опубликовано: **10.05.2010** Бюл. № 13(56) Список документов, цитированных в отчете о
поиске: **GB 2223614 A, 11.04.1990. RU 2121162 C1,
27.10.1998. US 2003/0176218 A1, 18.09.2003.
WO 03/025867 A2, 27.03.2003.**(85) Дата перевода заявки РСТ на национальную
фазу: **05.05.2006**(86) Заявка РСТ:
US 2004/032867 (06.10.2004)(87) Публикация РСТ:
WO 2005/036473 (21.04.2005)Адрес для переписки:
**125040, Москва, Ленинградский пр-т, 23,
Патентно-лицензионная фирма
"Транстехнология", пат.пов. Н.И.Золотых**

(72) Автор(ы):

**ПОЛСЕН Крэйг А. (US),
НГУЙЕН Бинх Т. (US)**(73) Патентообладатель(и):
АйДжиТи (US)**(54) СПОСОБ И СИСТЕМА ЗАЩИТЫ УНИВЕРСАЛЬНОГО КЛЮЧА**

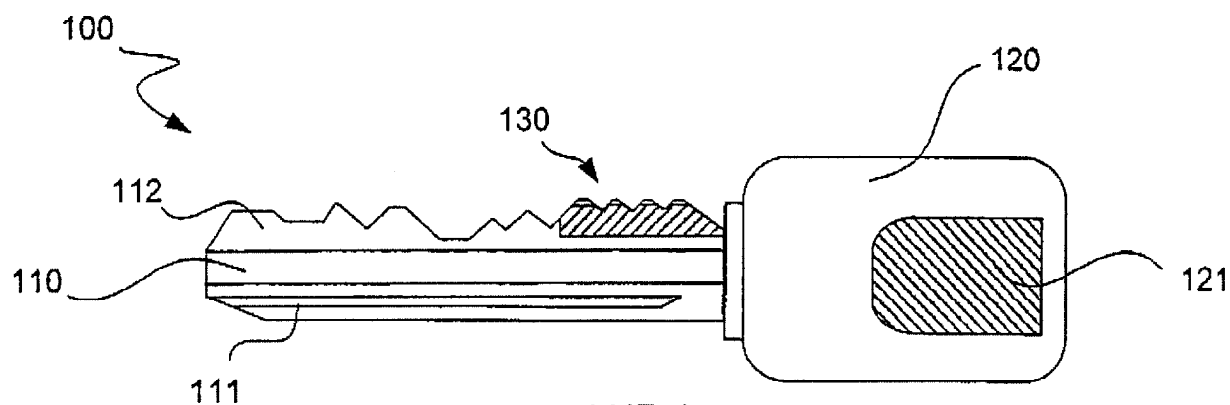
(57) Реферат:

Раскрываются способ обеспечения безопасности в игровой машине и игровая машина, разрешение на доступ к которой обеспечивается посредством выполнения этапов: вставления механического ключа в электромеханический замок; считывания первого источника идентификационных признаков с ключа, где указанный первый источник идентификационных признаков содержит информацию или данные, специфические для указанного замка; считывания второго источника идентификационных признаков, где указанный

второй источник идентификационных признаков содержит информацию, специфическую для одного или более пользователей ключа; анализа второго источника идентификационных признаков, относящегося к хранимому файлу с биометрической информацией в местонахождении, отдельном от указанного механического ключа; авторизации использования ключа по результатам считывания обоих идентификационных признаков; ограничения доступа к указанной области с возможностью доступа по ключу по выбору на основе одного или более

дополнительных факторов; и автоматического разрешения или отклонения доступа к указанной области с возможностью доступа по ключу в соответствии с решением на этапе

авторизации. Технический результат - повышение безопасности работы игровой машины. 3 н. и 14 з.п. ф-лы, 12 ил.



ФИГ. 4

RU 2389076 C2

RU 2389076 C2



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION(21), (22) Application: **2006115366/09, 06.10.2004**(24) Effective date for property rights:
06.10.2004(30) Priority:
09.10.2003 US 10/605,574(43) Application published: **20.11.2007**(45) Date of publication: **10.05.2010 Bull. 13**(85) Commencement of national phase: **05.05.2006**(86) PCT application:
US 2004/032867 (06.10.2004)(87) PCT publication:
WO 2005/036473 (21.04.2005)

Mail address:
**125040, Moskva, Leningradskij pr-t, 23, Patentno-
litsenzionnaja firma "Transtekhnologija",
pat.pov. N.I.Zolotych**

(72) Inventor(s):

**POLSEN Krehjg A. (US),
NGUJEN Binkh T. (US)**

(73) Proprietor(s):

AjDzhiTi (US)

(54) METHOD AND DEVICE FOR PROTECTING UNIVERSAL KEY

(57) Abstract:

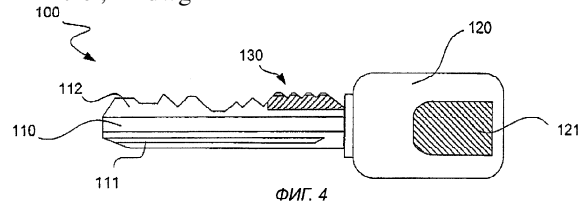
FIELD: information technology.

SUBSTANCE: disclosed is a method of ensuring safety in a game machine and a game machine which can be accessed through the following steps. Inserting a mechanical key into an electromechanical lock. Reading a first source of identification features from the key, where the said first source of identification features contains information or data which are specific for the said lock. Reading a second source of identification features, where the said second source of identification features contains information which is specific for one or more key users. Analysis of the second source of identification features relating to the stored file with biometric information in a location separate from the said mechanical key. Authorisation of using

the key depending on the results from reading both identification features. Barring access to the said area with possibility of accessing the key selectively, based on one or more additional factors, and automatic granting or barring access to the said area with possibility of accessing the key in accordance with the permission at the authorisation step.

EFFECT: more secure operation of the game machine.

17 cl, 12 dwg



ОБЛАСТЬ ТЕХНИКИ, К КОТОРОЙ ОТНОСИТСЯ ИЗОБРЕТЕНИЕ

Настоящее изобретение относится, в общем, к способу и устройству для обеспечения защиты и, в частности, к способу и устройству для обеспечения защищенного доступа к устройству типа игровой машины по ключу.

ПРЕДПОСЫЛКИ К СОЗДАНИЮ ИЗОБРЕТЕНИЯ

В ответ на современные технологические достижения и изменяющиеся потребности в делах защиты собственности, противодействия криминалу и предотвращения нежелательного и несанкционированного доступа во многих домах и коммерческих учреждениях типа банков, универмагов, ювелирных магазинов, торговых центров, школ, казино и других игровых заведений теперь обычно устанавливаются все более и более сложные замки и замковые устройства. Такие замки и замковые устройства позволяют предотвратить нежелательный доступ к самым различным зонам и устройствам, главным образом при использовании в сочетании с дополнительными мерами безопасности. Хотя защищенный доступ может быть желательным в отношении лиц или вещей, физически бывающих в заданном помещении типа здания или комнаты, необходимость защищенного доступа может также возникать и в отношении содержимого различных устройств типа, например, сейфов, абонентских почтовых ящиков, шкафчиков, прилавков-витрин, САВ-файлов, электронного или компьютерного оборудования и различных других защищенных устройств. В отдельных случаях такое защищенное устройство может иметь многочисленные защищенные зоны с различными уровнями защиты и соответствующими требованиями для доступа к каждой зоне. Одним примером такого устройства с многоуровневой защитой может быть игровая машина (то есть слот-машина).

Так как казино и игровые заведения других форм представляют растущую многомиллиардную долларовую индустрию, в которой большие суммы денег могут быстро переходить из рук в руки во время многих типов проводимых на большой скорости игр, казино и другие игровые заведения являются главной мишенью для мошенничества и воровства и, таким образом, главным подходящим объектом для использования все большего числа инновационных и сложных устройств и систем защиты, которые могут включить в себя более новые замки и замковые устройства. Поскольку казино и другие игровые заведения в особенности часто используют сложные устройства и технические приемы защиты, казино и игровые машины, в общем, являются идеальным иллюстративным примером для типов замковых устройств и, в частности, способов и систем защиты универсальным ключом, рассматриваемых в данном документе. В соответствии с этим в приводимых ниже исследованиях и иллюстративных примерах по соображениям целесообразности рассматриваются прежде всего устройства и системы защиты казино и игровых машин, однако следует принимать во внимание, что такие системы и устройства защиты без труда могут быть использованы и применительно к другим типам учреждений, мест совершения действия и элементов.

Существует множество устройств, имеющих отношение к игровой машине, для которых могут требоваться различные уровни защиты. В качестве примеров устройств, для которых меры защиты могут быть отдельными и независимыми, можно назвать банкнотоприемники, монетоприемники или накопители монет, игровое СППЗУ или центральный процессор ("ЦП"), коммуникационные платы и другие. Многие такие устройства являются встроенными в игровую машину, хотя это не исключает возможности существования одного или более из них вне самой машины. Традиционно защитой обеспечивалась главная дверца игровой машины, и

эта защита представляла собой обычный механический ключ и замковое устройство. Дополнительные внутренние устройства в игровой машине типа упомянутых выше также часто обеспечивались защитой с идентичным или подобным обычным механическим ключом и замковым устройством. Устройства и способы обеспечения

5 доступа по ключу к зоне или устройству типа игровой машины в казино являются в общем известными, и варианты таких устройств и способов можно найти, например, в патентах США №4677834, 6125673 и 6604394, которые все включены в данный документ путем ссылки полностью и для всех целей.

10 Популярным в последнее время для многих игровых заведений стало также введение дополнительных настроек доступа, причем доступ по ключу к игровой машине или компоненту игровой машины в предпочтительном варианте сопровождается использованием идентифицирующей карточки типа карточки трекинга сотрудника. Такая карточка считывается после доступа к машине, так что

15 информация о сотруднике и другие транзакционные частности могут отмечаться и/или отслеживаться локально или на расстоянии. Использование такой карточки является главным образом информационным инструментальным средством, однако таким, что доступ к игровой машине и любому из ее внутренних отделений может продолжаться

20 до тех пор, пока лицо, запрашивающее доступ, будет иметь соответствующий механический ключ или ключи. Препятствием к использованию такой карточки также служит введение дополнительного этапа в процесс защищенного доступа, реализация которого может быть обременительной и вызывать неудобство.

25 Независимо от того, используется карточка или нет, для опытного похитителя несанкционированный доступ к игровой машине в некоторых случаях представляется возможным. Значительному упрощению такого доступ может также способствовать попадание ключа или набора ключей в нечестные руки. Среди некоторых примеров попадания ключей в нечестные руки можно привести кражу ключа, использование

30 утраченного ключа или несанкционированное дублирование ключа, в то же время в качестве других примеров можно назвать случаи, когда сотрудник казино, имеющий некоторый уровень защищенного доступа, увольняется или покидает место работы по иным причинам и не возвращает свои ключи, как это обычно требуется. Несмотря на дороговизну этого мероприятия, переоснащение всех банков или залов игровых

35 машин, в которых конкретный набор ключей был потерян или украден или в которых группа машин неоднократно становилась мишенью нападения со стороны лиц, которые имеют незаконный доступ к одному или более ключам, новыми замками является возможным.

40 Следовательно, существует необходимость в создании усовершенствованных способов и систем для предоставления защищенного доступа к зоне или устройству посредством механических ключей и замков и, в частности, в способах и системах, позволяющих устранить необходимость в карточке трекинга и создать лучшие

45 способы обеспечения гарантий против несанкционированного доступа к игровой машине, несмотря на наличие корректного механического ключа для той машины.

КРАТКОЕ ИЗЛОЖЕНИЕ СУЩНОСТИ ИЗОБРЕТЕНИЯ

Преимуществом настоящего изобретения является создание способа и устройства для защиты универсальным ключом, которые позволяют обеспечить более высокий

50 уровень защиты защищенной среды или объекта. Согласно одному варианту осуществления настоящего изобретения предлагаются способ и устройство, предусматривающие использование одного или более специально спроектированных замков и/или ключей в игровой машине, посредством которых удастся предотвратить

несанкционированный доступ к игровой машине, несмотря на наличие корректного ключа для этой конкретной машины. Достигается это путем проектирования замка, требующего для своего открывания одного или более дополнительных критериев в дополнение к физическому ключу. Такие дополнительные критерии могут включать в себя использование биометрической информации или ПИН-номера для авторизованного пользователя или других факторов помимо формы указанного ключа.

В одном конкретном варианте осуществления механический ключ используется в сочетании с электромеханическим замком, причем для открывания замка требуются как и вставление механического ключа и манипулирование этим ключом, так и отдельный электрический сигнал авторизации. Этот отдельный электрический сигнал может быть получен в результате корректного считывания биометрического параметра для авторизованного пользователя типа отпечатка пальца. В одном случае отпечаток пальца авторизованного пользователя может быть считан и утвержден устройством, встроенным непосредственно в механический ключ, после чего в электромеханический замок для разрешения доступа может быть послан сигнал положительной авторизации. В другом варианте изобретения отпечаток пальца может быть просто считан таким устройством внутри ключа, а данные могут быть посланы в механизм утверждения или внутри самой игровой машины или в каком-либо удаленном пункте, после чего сигнал положительной авторизации может быть передан в замок, если пользователь ключа является авторизованным лицом.

Согласно другому варианту осуществления настоящего изобретения предлагаются способ и устройство, предусматривающие использование одного или более альтернативных персональных идентификаторов в дополнение к механическому ключу. Такие персональные идентификаторы могут включать в себя цифровую наборную панель, требующую использования Персонального Идентификационного Номера или ПИНа, причем эта цифровая наборная панель может находиться на устройстве или рядом или на элементе, к которому требуется получить доступ, или на самом ключе. Таким образом, можно спроектировать механический ключ, содержащий один или более отличительных признаков, отображающихся на конкретном замке, который требуется открыть, типа формы и профиля конкретного ключа для корректного манипулирования механическими штырьками или рычагами внутри замка, а также один или более отличительных признаков, отображающихся на конкретном авторизованном пользователе, типа отпечатка пальца.

Другие способы, возможности и преимущества изобретения будут или станут очевидными для специалиста в данной области техники после изучения следующих ниже фигур и подробного описания. Предполагается, что все такие дополнительные способы, возможности и преимущества включены в это описание, не выходя за пределы объема изобретения и защищены прилагаемой формулой изобретения.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Чертежи приведены в иллюстративных целях и служат исключительно для объяснения примеров возможных конструкций и этапов процесса для раскрываемого заявленного интерфейса камеры безопасности. Эти чертежи никоим образом не ограничивают никаких изменений в форме и содержании изобретения, которые могут быть внесены специалистом в данной области техники, и не выходят за пределы существа и объема изобретения.

Фиг.1 - пространственное изображение типичной игровой машины согласно одному варианту осуществления настоящего изобретения.

Фиг.2 - пространственное изображение игровой машины, представленной на фиг.1, с открытой главной дверцей согласно одному варианту осуществления настоящего изобретения.

Фиг.3 - пространственное изображение типичного электромеханического замка согласно одному варианту осуществления настоящего изобретения.

Фиг.4 - вид сбоку типичного механического ключа со встроенным биометрическим устройством согласно одному варианту осуществления настоящего изобретения.

Фиг.5 - вид сбоку электрических контактов механического ключа, представленного на фиг.4, в увеличенном виде согласно одному варианту осуществления настоящего изобретения.

Фиг.6 - пространственное изображение альтернативного типичного электромеханического замка согласно одному варианту осуществления настоящего изобретения.

Фиг.7 - вид сбоку альтернативного типичного механического ключа с встроенным биометрическим устройством согласно одному варианту осуществления настоящего изобретения.

Фиг.8 - блок-схема конкретной считывающей системы защиты универсальным ключом с "несистемным управлением" согласно одному варианту осуществления настоящего изобретения.

Фиг.9 - блок-схема альтернативной считывающей системы защиты универсальным ключом с "системным управлением" согласно другому варианту осуществления настоящего изобретения.

Фиг.10 - блок-схема конкретной сетевой инфраструктуры для реализации способа и системы защиты универсальным ключом согласно одному варианту осуществления настоящего изобретения.

Фиг.11 - типичная база данных, содержащая ассоциированные идентификаторы данных различных авторизованных и утративших авторизацию лиц, согласно одному варианту осуществления настоящего изобретения.

Фиг.12 - блок-схема одного способа реализации способ и система защиты универсальным ключом согласно одному варианту осуществления настоящего изобретения.

ПОДРОБНОЕ ОПИСАНИЕ

В этом разделе описывается пример применения способа и системы, соответствующих настоящему изобретению. Пример приведен исключительно с целью внесения дополнительного смысла и помощи в понимание предмета изобретения.

Поэтому специалисту в данной области техники должно быть очевидно, что настоящее изобретение может быть осуществлено без некоторых или всех этих особенностей. В других случаях подробное описание известных этапов процесса было опущено, чтобы излишне не затруднять выявления предмета настоящего изобретения. Возможны и другие применения, так что предлагаемый пример не должен рассматриваться как ограничение.

Следующее ниже подробное описание ведется со ссылками на прилагаемые чертежи, которые формируют часть описания и на которых в качестве иллюстрации представлены частные варианты осуществления настоящего изобретения. Варианты осуществления описаны достаточно подробно, чтобы обеспечить специалисту в данной области техники возможность реализовать изобретение на практике, однако следует понимать, что эти варианты не являются ограничением; так что возможно использование других вариантов осуществления и внесение изменений, не выходящих

за пределы существа и объема изобретения.

Одним преимуществом настоящего изобретения является создание способа и устройства для защиты универсальным ключом, которые позволяют обеспечить более высокий уровень защиты защищенной среды или объекта. В одном варианте осуществления настоящего изобретения предлагаются один или более специально спроектированных замков и/или ключей, посредством которых удастся предотвратить несанкционированный доступ к зоне или устройству, несмотря на наличие корректного ключа для этой конкретной зоны или устройства. Достигается это путем проектирования замка, требующего для своего открывания одного или более дополнительных критериев в дополнение к физическому ключу. Такие дополнительные критерии могут включать в себя использование биометрической информации или ПИН-номера для авторизованного пользователя или других факторов помимо формы указанного ключа.

Как было указано выше, несмотря на то что способ и система защиты универсальным ключом, предлагаемые в данном изобретении, описываются со ссылками и иллюстрациями, касающимися прежде всего игровых заведений и игровых машин, эту систему можно без труда адаптировать применительно к другим видам бизнеса и сред, так что ее использование не ограничивается исключительно игровыми машинами или игровыми заведениями. Если продолжить далее иллюстрировать способ и систему защиты универсальным ключом на примере казино или другого игрового заведения, то нужно отметить, что такие учреждения служат главными мишенями для воров, мошенников и других различных криминальных личностей как снаружи, так и "внутри". В частности, слот-машины и другие игровые машины являются предпочтительными объектами большинства типов совершаемых хищений и мошенничеств по ряду причин. Поэтому игровые машины являются особенно подходящими устройствами для иллюстрации функций и возможностей предлагаемых способа и системы, раскрываемых в этом документе.

На фиг.1 представлено пространственное изображение типичной игровой машины согласно одному варианту осуществления изобретения. Игровая машина 10 включает в себя приставку 11 и основной корпус 12, который, как правило, окружает внутреннюю часть машины (не показано) и который доступен взгляду пользователей. Со своей передней стороны основной корпус 12 имеет главную дверцу 20, открывающуюся для обеспечения доступа внутрь машины. На поверхность главной дверцы обычно выведен один или более переключателей или кнопок 21 ввода для игрока, одно или более устройств приема денег или кредитов, типа монетоприемника 22 и банкното- или билетоприемника 23, лоток 24 для монет и защитное стекло 25. Через главную дверцу 20 можно видеть основной монитор с видеодисплеем 26 и одну или более информационных панелей 27. Основной монитор с видеодисплеем 26, как правило, представляет собой катодно-лучевую трубку, плоскопанельный жидкокристаллический (ЖК) дисплей с высоким разрешением, плазменный/светодиодный дисплей или другой обычный видеомонитор с электронным управлением. Приставка 11, которая обычно установлена на верхней поверхности основного корпуса 12, может также содержать банкното- или билетоприемник 28, малую клавишную панель 29, один или более дополнительных дисплеев 30, считыватель 31 карточек, один или более динамиков 32, одну или более камер 33 и вспомогательный монитор с видеодисплеем 34, который также может представлять собой катодно-лучевую трубку, плоскопанельный ЖК-дисплей с высоким разрешением, плазменный/светодиодный дисплей или другой обычный

видеомонитор с электронным управлением. Возможны также другие компоненты и комбинации в случае возможности размещения одного или более компонентов, традиционно зарезервированных для основного корпуса, в приставке и наоборот.

Игровая машина 10 также включает в себя одно или более замковых устройств, спроектированных для ограничения доступа в игровую машину. Такие устройства могут содержать механические или электромеханические замки, требующие использования одного или более ключей, и в предпочтительном варианте по меньшей мере один замок должен быть с возможностью доступа по ключу в каком-либо месте на внешней стороне машины. Такими замками могут быть, например, замки с нарезкой, с бородками, под ключ-жест, цилиндровые, со штырьковым реверсивным механизмом, сувальдные, трубчатые, замки для торговых автоматов и замки самого обычного типа, а также замок любого другого типа по желанию. Точно так же такими ключами могут быть, например, ключи с бородкой, ключи-жесты, плоские, трубчатые, цилиндрические и ключи трубчатого типа, а также ключ любого другого типа по желанию. Как показано на фиг.1, замок главной дверцы содержит по меньшей мере одну личинку на внешней поверхности машины типа, например, личинки 41, в которую может быть вставлен ключ для разблокировки и открывания главной дверцы 20. Кроме того, доступ к одному или более внутренним компонентам машины может быть обеспечен прямо с внешней стороны машины, например, через внешнюю защитную дверцу 50, снабженную замком с личинкой 51 также на внешней поверхности машины. Подобным же образом прямой доступ с внешней стороны машины можно получить и к дополнительным компонентам машины, не показанным на фигуре. В другом варианте изобретения для доступа к одному или более внутренним компонентам машины может потребоваться преодоление более одного уровня доступа, например, перед разблокировкой и получением доступа к внутреннему компоненту машины возникает необходимость разблокировки и открытия главной дверцы 20.

На фиг.2 игровая машина, показанная на фиг.1, представлена с открытой главной дверцей. В дополнение к внешним элементам, описанным выше, типа приставки 11, основного корпуса 12 и основного монитора с видеодисплеем 26, игровая машина 10 также содержит множество внутренних компонентов. Среди таких компонентов можно назвать, например, монетоприемник 35, механизмы 42 и 43 блокировки главной дверцы, обратную сторону защитной дверцы 50 и ряд других элементов, не перечисленных по соображениям нецелесообразности. Механизмы 42 и 43 блокировки главной дверцы содержат систему механической блокировки, состоящую из стандартного стержня с крюками и гнездами под эти крюки, причем перемещение стержня 42 с крюками вверх и вниз для блокировки и разблокировки главной дверцы 20 обеспечивается путем соответствующих манипуляций с личинкой 41. Эта частная система механической блокировки была рассмотрена в иллюстративных целях, однако следует понимать, что эта показанная на фигуре система может быть заменена на любую другую стандартную систему блокировки, если другие такие системы блокировки также приведут к созданию объектов и достижению целей раскрываемых в данном документе способов защиты универсальным ключом.

Как показано на фиг.2, внутри игровой машины 10 также имеется ряд дополнительных защищенных отсеков, снабженных замками с личинками. Например, внутренний банкнотоприемник 60 содержит бокс для хранения банкнот, запертый на замок с личинкой 61. Защищенный отсек 70 для электроники также содержит бокс для ЦП машины и/или других важных электронных компонентов, запертый на замок с

личинкой 71. Среди других внутренних компонентов, не показанных на фигуре, можно назвать монетоприемник, накопитель монет или электронную коммуникационную плату, которые могут быть защищены аналогичным образом. При такой защите для получения доступа к одному или более внутренних отсеков, каждый из которых в предпочтительном варианте характеризуется требованиями по доступу, отличными от таковых для главной дверцы 20 и каждого другого внутреннего отсека, необходимо не только открыть главную дверцу 20 игровой машины, но нужно также преодолеть дополнительное защитное средство или приспособление. В другом варианте изобретения, как указано выше, прямой доступ к одному или более внутренним компонентам можно получить не обязательно через главную дверцу 20. В одном таком примере доступ к внутреннему банкнотоприемнику 60 можно получить в результате открытия внешней защитной дверцы 50 через личинку 51 и внутреннего банкнотоприемника 60 через личинку 61, в то время как главная дверца остается закрытой.

На фиг.3 представлено пространственное изображение типичного электромеханического замка согласно одному варианту осуществления настоящего изобретения. Электромеханический замок 40 содержит механический замок цилиндрического типа, имеющий личинку 41, один или более соответствующих механизмов 42 блокировки, внешний корпус 44 и один или более электрических соединителей 45. Как было указано выше, соответствующее управление механизмом 42 блокировки и его движение обеспечиваются в результате успешных манипуляций с замком, осуществляемых в предпочтительном варианте через личинку 41 с помощью авторизованного ключа авторизованным пользователем. В предпочтительном варианте осуществления успешное манипулирование с замком 40 невозможно без использования подходящего механического ключа и поступления разрешающего электрического сигнала. Этот разрешающий электрический сигнал можно послать в замок от внешнего источника через соединитель 45 или можно генерировать полностью внутри замка, личинки и/или самого ключа. В другом варианте изобретения для передачи разрешающего сигнала может быть использован любой тип беспроводной связи, например, беспроводная передача данных по радиоканалу ("Wi-Fi") в системе Bluetooth® Wireless, использующей стандарт IEEE802.1x или другую подобную стандартную сетевую технологию. В случае наличия механического ключа и поступления разрешающего электрического сигнала один или более соленоидов или других исполнительных механизмов внутри электромеханического замка активизируются, обеспечивая тем самым возможность успешного манипулирования механизмом 42 блокировки.

При таком благоприятном состоянии в случае наличия корректного ключа и поступления разрешающего электрического сигнала пользователь получает возможность поворота личинки 41 и последующего вращения ключа внутри личинки, обеспечивающего управление механизмом блокировки. В другом варианте изобретения конструкцией замка 40 может быть предусмотрена возможность поворота соответствующего механического ключа внутри личинки в любой момент времени, за исключением случая, когда соответствующий соленоид или исполнительный механизм внутри замка не активизируется без поступления соответствующего разрешающего электрического сигнала. Способы и устройства с использованием соленоидов или других исполнительных механизмов внутри электромеханического замка хорошо известны специалистам в данной области техники и, в частности, предполагается, что любой такой подходящий способ или

устройство могут быть использованы в патентуемых способах и системах защиты универсальным ключом, предлагаемых в данном документе.

Описание одного примера усовершенствованного электромеханического замка и системы, которые могут быть использованы в сочетании с игровыми машинами, и, в частности, с настоящим изобретением, приводится в переданной в общее пользование и совместно рассматриваемой заявке №09/824621 на патент США, поданной Mattice с соавт. 2 апреля 2001 г. под названием "Method and Apparatus for Controlling Access to Areas of Gaming Machines" ("Способ и устройство для контроля за доступом к зонам игровых машин"), положения которой включены в данный документ полностью для всех целей. Другой типичный пример использования механического ключа и другой информации в сочетании с игровыми машинами и системами описывается в переданном в общее пользование патенте США №6439996, опубликованном LeMay с соавт. 27 августа 2002 г. под названием "Key for a Gaming Machine and Method of Use Thereof" ("Ключ для игровой машины и способ его использования"), который также включен в данный документ полностью и для всех целей. Как показывается в данном документе, использование предлагаемого электромеханического замка и системы в предпочтительном варианте обеспечивается внутри игровой машины или системы с помощью специфических данных или информации типа биометрической информации. Другой пример биометрической информации, используемой в сочетании с игровыми машинами и системами, описывается в переданной в общее пользование и совместно рассматриваемой заявке №09/491899 на патент США, поданной 27 января 2000 г. Wells с соавт. под названием "Игровой терминал и система с биометрической идентификацией" ("Gaming Terminal and System with Biometric Identification"), положения которой также включены в данный документ полностью и для всех целей.

На фиг.4 представлен вид сбоку типичного механического ключа с встроенным биометрическим устройством согласно одному варианту осуществления настоящего изобретения. Механический ключ 100 представляет собой цилиндрический ключ, имеющий профилированный компонент 110 и рукоятку 120. Профилированный компонент 110 в предпочтительном варианте выполнен из твердого металла или пластика, такого чтобы сохранить форму и профиль этого компонента с течением времени практически неизменными. Дальнейшее обсуждение проблемы в данном документе будет вестись в предположении, что этот компонент сделан из металла и, в частности, из стали, что не исключает возможности использования и множества других подходящих материалов. Этот металлический участок ключа включает в себя один или более идентификационных признаков, которые могут "считываться" замком для определения, является ли ключ корректным для этого замка или нет. Среди таких идентификационных признаков можно назвать ряд характеристик типа системы бороздок, бокового профиля, одного или более краевых профилей и/или полной физической формы ключа.

Специфическая форма 111 ключа, которая является по существу комбинацией бокового профиля и системы бороздок для профилированного компонента 110, обычно используется во многих типах металлических ключей. Этот боковой профиль и система бороздок по существу обеспечивают возможность физического вставления ключа в замки определенных типов, в том числе в замок, для которого ключ предназначен, и предотвращают возможность вставления в замки большинства других типов. Боковой профиль может включить в себя множество углублений, сформированных вдоль профилированного компонента 111, а также любое число изгибов и поворотов, часто между 3 и 7. Каждое углубление и каждый изгиб или

поворот профиля могут работать как отдельный признак для обеспечения отличия одного ключа 100 от многих других ключей. В соответствии с этим специфическая форма или побочный профиль 111 являются одним источником идентификационных признаков, содержащим информацию или данные, специфические для замка, обеспечивающего возможность считывания ключа 100. Профилированный или металлический компонент 110 также включает в себя по меньшей мере один и иногда два краевых профиля 112, используемых для манипулирования штырьками и/или рычагами внутри реверсивного механизма замка или другой внутренней структуры замка. Каждое возвышение, каждый спуск, зубец, каждая впадина и каждое плато по краевому профилю могут работать как отдельный признак для ключа 100, так что краевой профиль 112 является другим источником идентификационных признаков, содержащим информацию, специфическую для замка, обеспечивающего возможность считывания ключа 100. Специалисту в данной области техники очевидно, что если ключ 100 является действительно корректным ключом для данного замка, то специфическая форма 111 этого ключа позволит вставить его в этот замок, а краевой профиль 112 ключа - нажать на все необходимые штырьки и/или рычаги внутри замка в корректных для доступа положениях, что обеспечит "считывание" ключа замком как корректного.

Рукоятка 120 ключа может быть выполнена из того же самого материала, что и остальная часть ключа, но в предпочтительном варианте - из пластика, полимера или другого жесткого электроизоляционного материала. Согласно одному варианту осуществления настоящего изобретения, рукоятка 120 включает в себя по меньшей мере одно биометрическое устройство 121, которое в предпочтительном варианте встроено внутрь рукоятки и в предпочтительном варианте является датчиком отпечатков пальцев. Такой датчик отпечатков пальцев может представлять собой, например, MBF300 Fingerprint Sweepsensor™ производства компании Fujitsu, Ltd. (Токио, Япония) или EntrePad AES3400 или AES2500 Fingerprint Sensors производства компании AuthenTec, Inc (Мельбурн, Флорида), хотя возможно эффективное использование датчиков отпечатков пальцев и других торговых марок и типов. В предпочтительном варианте этот датчик отпечатков пальцев спроектирован для считывания одного или более критических участков отпечатка пальца, обеспечивающих возможность принятия решения о том, действительно ли пользователь ключа является авторизованным пользователем. Специалистам в данной области техники хорошо известны технические приемы электронного считывания, анализа и распознавания отпечатков пальцев, и любая такая технология рассматривается как пригодная для использования в настоящем изобретении. Следовательно, отпечаток пальца или другая форма биометрических данных представляет собой один источник идентификационных признаков, содержащих информацию или данные, специфические для конкретного пользователя ключа 100.

Решение о том, является ли считанный отпечаток пальца действительно авторизованным, может быть принято любым возможным путем, например, с помощью микропроцессора или другого процессора внутри самого датчика отпечатков пальцев или встроеного куда-то в другое место рукоятки ключа или удаленного процессора, с которым датчик отпечатков пальцев обменивается информацией, относящейся к считываемому отпечатку пальца. Использование таких удаленных способов проведения анализа и принятия решения может быть желательным по ряду причин. Например, затраты на установку микропроцессора в рукоятку ключа могут быть существенными, а сам ключ при этом может становиться

более уязвимым. Кроме того, в случае, когда профиль обрабатываемого с помощью ключа сигнала допускает прерывание и/или имитацию соответствующего сигнала авторизации, вырабатываемого самим ключом, для мошенников или похитителей могут возникать дополнительные возможности по совершению мошеннических действий по отношению к системе. И наоборот, конструкция, в которой на ключе установлен только датчик отпечатков пальцев, а анализ и авторизация выполняются на удаленном процессоре, вероятно будет иметь больше гарантий против взлома и мошенничества. В любом случае предпочтительнее пересылать и/или принимать электрические сигналы от ключа 100 в процессе обмена данными и/или статусом авторизации при считывании отпечатков пальцев на рукоятке ключа, причем передача таких электрических сигналов может осуществляться посредством электрической контактной области 130 ключа, системы Wi-Fi-типа или другой беспроводной системы или другого средства связи по желанию. Кроме того, любые передаваемые данные и/или сигналы авторизации или статус предпочтительнее подвергать шифрованию с помощью любых доступных программ или систем шифрования.

В приведенном выше иллюстративном примере была рассмотрена биометрия отпечатка пальца, однако должно быть очевидно, что и другие формы биометрической информации могут быть использованы вместо или в сочетании с отпечатком пальца. Среди примеров таких дополнительных биометрических характеристик можно назвать черты лица, для которых существуют программы распознавания лиц, голосовые тоны и особенности, для которых существуют программы распознавания речи, и узоры сетчатки глаза, для которых существуют специальные сканеры. Любой из них или из множества других биометрических индикаторов может быть использован в предлагаемых способе и системе защиты универсальным ключом, чтобы обеспечить такое их применение, в соответствии с которым некоторая конкретная биометрическая характеристика авторизованного пользователя ключа запоминается и используется для сравнения с впоследствии считываемой биометрической характеристикой пользователя ключа, предпринимающего попытку получения доступа, и верификации легитимности этого пользователя.

В другом варианте изобретения для получения идентификационных признаков, специфических для одного или более авторизованных пользователей ключей, может быть использован небиометрический информационный источник. Такой небиометрический информационный источник может содержать, например, цифровую, алфавитную и/или символьную наборную панель, адаптированную для приема персонального идентификационного номера ("ПИНа") или подобного кода доступа. В одном варианте осуществления такая наборная панель может представлять собой обычную 10-клавишную цифровую панель, при использовании которой ПИН человека может быть любым числовым кодом в виде подходящей последовательности цифр, количество которых в предпочтительном варианте составляет от четырех до десяти, хотя не исключаются как более короткие, так и более длинные последовательности. В предпочтительном варианте авторизованный ПИН известен только конкретному пользователю или ограниченной группе пользователей, так что ввод авторизованного ПИНа соответственно отражает идентификационные признаки, которые являются специфическими для одного или более авторизованных пользователей ключа. Реальная наборная панель может быть миниатюрной и размещена на самом механическом ключе или, в другом варианте изобретения, может быть установлена в электромеханическом замке, который требуется открыть, или

рядом. Место установки может находиться на объекте, доступ к которому требуется получить, типа игровой машины или на каком-либо другом легкодоступном соседнем устройстве, стене или другой структуре. Считыватели для других идентификационных признаков типа датчиков отпечатков пальцев, систем детектирования речевого сигнала или устройств сканирования радужной оболочки глаза могут быть
5 размещены подобным же образом в электромеханическом замке, который требуется открыть, или рядом.

Другой элемент, который может быть использован для создания специфических идентификационных признаков, используемых в способах и системах защиты
10 универсальным ключом, предлагаемыми в данном документе, является тэгом радиочастотной идентификации ("RFID"). Тэг RFID, как правило, представляет собой крошечную микросхему, запрограммированную на содержание конкретной информации, в соответствии с чем такая информация может передаваться после
15 приема соответствующего радиочастотного ("РЧ") сигнала. Для обеспечения приема и передачи РЧ сигналов обычно к тэгу RFID крепится одна или более антенн, и полный размер типичного тэга RFID сравним с размером зернышка перца. Использование тэгов RFID можно сравнить с использованием стандартных штрих-кодов UPC и
20 сканеров, однако большинство тэгов RFID может хранить на порядок больший объем информации, чем штрих-код, и не требует ни прямой видимости, ни удовлетворения других физических факторов для активизации и считывания устройством считывания тэгов, осуществляющих испускание и прием РЧ-сигналов.

В настоящем изобретении один или более тэгов RFID может быть использован для
25 того, чтобы создать источник идентификационных признаков для используемого механического ключа. Такие идентификационные признаки в предпочтительном варианте используются в дополнение к одному или более других источников идентификационных признаков, рассмотренных выше. В таком примере
30 использования тэга RFID тэг RFID может быть запрограммирован на наличие наборного кода и такой тэг в предпочтительном варианте может быть встроен внутрь соответствующего механического ключа 100. Считыватель тэга RFID может быть размещен внутри интересующей игровой машины или недалеко от нее, так что считыватель тэга будет испускать РЧ-сигнал по меньшей мере тогда, когда
35 механический ключ вставлен в замок игровой машины. Если тэг RFID, встроенный внутрь механического ключа, после активизации вырабатывает соответствующий код и этот код затем считывается считывателем тэга, то после этого может быть осуществлена пересылка авторизующего сигнала из считывателя в
40 электромеханический замок. В предпочтительном варианте замок спроектирован так, что будет открываться только после приема такого авторизующего сигнала. Такая адаптация является полезной в случаях, когда кто-нибудь, например, сделал попытку создать незаконные копии механического ключа, которые не работали бы должным образом без внедренного тэга RFID, содержащего корректно запрограммированный
45 код.

Точно также электромеханический замок, использующий какие-либо соответствующие биометрические или небιοметрические источники
идентификационных признаков, специфических для пользователя, в предпочтительном
50 варианте не срабатывает до тех пор, пока авторизующий сигнал не поступит в замок из какого-либо устройства или устройства не проведут измерения и анализа таких специфических для пользователя идентификационных признаков, чтобы подтвердить присутствие авторизованного пользователя. Такие анализирующие устройства

анализа могут быть выполнены в виде микропроцессора или процессора внутри самого ключа или в виде отдельных модулей внутри замка или удаленных от замка. Такие отдельные модули могут принимать форму, например, цифровых наборных панелей со встроенным микропроцессором, аналитического модуля внутри самого электромеханического замка или удаленного модуля, участвующего в обмене информацией с замком. Такой удаленный модуль может быть частью сети, посредством которой централизованный универсальный сервер или специализированный сервер защиты может быть использован для регулирования и проведения мониторинга множества элементов защиты, в том числе доступа к ряду игровых машин. Ниже приводится дальнейшее более подробное описание такой системы, а также одного из средств обеспечения электрической связи между механическим ключом и соответствующим замком и/или системой.

Таким образом, управляющий типа оператора казино может обеспечить значительно более высокий уровень контроля за системами блокировки и соответствующими им распределенными механическими ключами. В случае потери или кражи одного или более ключей такие ключи не могут быть, по-видимому, использованы никем, несмотря на то что этот ключ можно физически вставить в определенный замок или замки. Поскольку неавторизованный пользователь, по-видимому, будет не в состоянии удовлетворить запрос, связанный с замком, относительно того, является ли этот пользователь авторизованным или нет, то простого владения ключом, как правило, будет недостаточно для предоставления доступа к интересующей защищенной среде. Следовательно, владельцам казино и другого бизнеса не потребуется переоснащать многие машины новыми замками и выпускать новые ключи всякий раз при возникновении проблемы с одним или более механическими ключами. Можно предположить, что достигаемая в результате долговременная экономия времени и денег, не требующая таких действий, будет существенной.

На фиг.5 представлен вид сбоку области 130 электрических контактов механического ключа, изображенного на фиг.4, в увеличенном виде. Эта область механического ключа представляет собой по меньшей мере один пример обеспечения электрической связи между ключом и электромеханическим замком и/или сетью защиты. Как было указано выше, профилированный компонент 110 ключа в предпочтительном варианте выполнен из металла или жесткого пластика, подходящего для формирования типичных форм, а также боковых и краевых профилей в механических ключах. Вставка 131 в предпочтительном варианте крепится к остальной части ключа в углублении или на другом определенном участке профилированного компонента 110, примыкающего к рукоятке ключа. Такое крепление может быть получено с помощью запрессовки, склеивания, сварки, с помощью эпоксидной смолы или другого подходящего крепежного средства. Над вставкой 131 выполнены один или более электрических контактов 132-135, используемых для подачи питания и/ли передачи одного или более электрических сигналов на ключ и от ключа. Вследствие необходимости размещения многочисленных электрических выводов в границах небольшого пространства вставку 131 предпочтительнее выполнять из электроизоляционного материала типа пластика, полимера, кварца или стекла, например, по меньшей мере с одним внутренним электрическим проводом или выводом (не показанным), идущим от каждого электрического контакта через вставку в направлении к электрическому контакту (не показанному) на краю рукоятки, примыкающей к вставке.

Электрические контакты 132-135 размещены так, что каждый вступает в контакт с определенным электрическим контактом внутри реверсивного механизма или другого внутреннего компонента электромеханического замка, когда ключ полностью вставлен в замок. Отдельные выводы или провода, подключенные к каждому внутреннему контакту внутри замка, затем вступают в контакт с одним или более подходящим электронным распределительным и/или аналитическим модулем с возможностью обработки электрических сигналов, пересылаемых от ключа. В настоящем типичном варианте осуществления предложено ровно четыре электрических контакта 132÷135, однако очевидно, что возможно также использование большего или меньшего числа контактов, и размещаться эти контакты могут в любом порядке и в любых положениях по желанию. Предпочтительными являются электрические контакты USB-типа, однако не исключаются и контакты другого стандарта или заказные контакты. В этом конкретном варианте осуществления контакты 132 и 133 могут быть спроектированы для передачи данных от ключа (и также возможно на ключ), в то время как контакты 134 и 135 являются контактами "питания", посредством которых на ключ может подаваться электроэнергия для управления датчиком отпечатков пальцев и микропроцессором в случае его применения. В другом варианте изобретения ключ может содержать батарею, обеспечивающую подачу питания от ключа в замок через контакты питания на ключе. В таком случае замок может не иметь никакого источника питания, кроме имеющегося в ключе.

В одном варианте осуществления механический ключ не включается вплоть до поступления питания через контакты 132 и 133 питания от механического замка, в который этот ключ вставлен. После этого встроенный датчик отпечатков пальцев считывает отпечаток пальца человека, держащегося за рукоятку ключа вне замка, и или обрабатывает и анализирует эту информацию непосредственно возможно с помощью микропроцессора или процессора, также размещенного внутри рукоятки ключа, или пересылает данные по отпечатку пальца через контакты 134 и 135 данных для их обработки замком или удаленной обработки. При локальной обработке и анализе данных отпечатка пальца аутентификацию данных пользователя называют аутентификацией с "несистемным управлением". В таких случаях управляющий файл с данными по корректному отпечатку пальца в предпочтительном варианте хранится в одном или более блоках памяти внутри рукоятки ключа, так что локальный микропроцессор или микропроцессор в рукоятке ключа могут без труда обращаться к этому управляющему файлу по требованию, сравнивать данные по текущему отпечатку пальца на датчике, подтверждать или не подтверждать совпадение и посылать сигнал авторизации на замок через контакты 134 и 135 данных. Такой сигнал авторизации может быть простым сигналом включения или выключения, и в этом случае для его отправки требуется только один контакт данных, или может представлять собой сигнал, до некоторой степени закодированный в виде импульсов, распространяющихся в направлении одного, двух или более контактов таким образом, что он может считываться замком, что делает успешность попыток взлома и мошенничества в отношении системы существенно менее вероятной.

В альтернативном варианте изобретения замок может содержать свой собственный источник питания, в то время как механический ключ может содержать внутреннюю батарею, так что контакты питания не являются обязательными. В качестве другой альтернативы от контактов данных можно также отказаться в пользу ключа и системы блокировки, которые обмениваются данными полностью через РЧ-сигналы.

При таком варианте осуществления может использоваться относительно сложный тэг RFID, или микропроцессор, или микропроцессор в сочетании с РЧ-приемопередатчиком. В таком варианте осуществления, как было указано выше, возможно использование любого типа Wi-Fi, Bluetooth® или другой беспроводной связи. В случае механического ключа, имеющего внутреннюю батарею и использующего РЧ-технологии, для передачи данных электрические контакты могут вообще не потребоваться. Когда анализ и аутентификация предложенного отпечатка пальца не должны выполняться внутри самого механического ключа, аутентификацию данных пользователя называют аутентификацией с "системным управлением". В таких случаях выполнение одного или более этапов анализа или аутентификации может осуществляться внутри действующего электромеханического замка или рядом или в каком-либо удаленном пункте, например, сети на основе сервера, как это описывается более подробно ниже.

На фиг.6 представлено пространственное изображение альтернативного типичного электромеханического замка согласно одному варианту осуществления настоящего изобретения. Электромеханический замок 40А в значительной степени походит на электромеханический замок 40, представленный на фиг.3, за исключением того, что замок 40А представляет собой механический замок трубчатого типа, имеющий трубчатую личинку 41А в дополнение к одному или более соответствующих механизмов 42 блокировки, внешнему корпусу 44 и одному или более соединителей 45. Как и в примере, рассмотренном выше, соответствующее управление механизмом 42 блокировки и его движение обеспечиваются в результате успешных манипуляций с замком в предпочтительном варианте через личинку 41А с помощью авторизованного ключа авторизованного пользователя. Точно так же разрешающий электрический сигнал можно послать в замок от внешнего источника через соединитель 45 или можно генерировать полностью внутри замка, личинки и/или самого ключа, причем для такой связи может быть использован альтернативный тип связи, например Bluetooth® и другие системы Wi-Fi.

На фиг.7 представлен вид сбоку альтернативного типичного механического ключа с встроенным биометрическим устройством согласно одному варианту осуществления настоящего изобретения. Механический ключ 150 содержит трубчатый ключ, имеющий профилированный компонент 160 и рукоятку 170. Как и в варианте, рассмотренном ранее, профилированный компонент 160 предпочтительнее выполнять из твердого металла или пластика, такого, чтобы можно было сохранить форму и профиль этого компонента с течением времени практически неизменными. Этот профилированный компонент 160, который является обычно цилиндрическим и полым, включает в себя один или более физических признаков типа отдельных вырезов или бороздок 161 и/или зубцов или направляющих 162, комбинация которых может физически "считываться" замком для определения, является ли конкретный трубчатый ключ корректным для этого замка или нет. Точно так же рукоятка 170 может быть выполнена из пластика, полимера или другого жесткого электроизоляционного материала. Согласно одному варианту осуществления настоящего изобретения рукоятка 170 включает в себя по меньшей мере одно биометрическое устройство 171, которое в предпочтительном варианте встроено внутрь рукоятки и в предпочтительном варианте является датчиком отпечатков пальцев, примеры и функциональные возможности которого рассмотрены выше. Как и в предшествующем примере, отпечаток пальца или другая форма биометрических данных, таким образом, представляет собой один источник идентификационных

признаков, содержащих информацию или данные, специфические для конкретного пользователя ключа 150.

Также подобно предшествующему примеру предпочтительнее пересылать и/или принимать один или более электрических сигналов от ключа 150 в процессе обмена данными и/или статусом авторизации при считывании отпечатков пальцев на рукоятке ключа. Передача таких электрических сигналов может осуществляться посредством электрической контактной области 180 ключа, системы Wi-Fi-типа или другой беспроводной системы или другого средства связи по желанию, причем любые передаваемые данные и/или сигналы авторизации или статус предпочтительнее подвергать шифрованию с помощью любых доступных программ или систем шифрования. Электрическая контактная область 180 может в значительной степени походить на электрическую контактную область 130 в предшествующем примере или может быть изменена по желанию, чтобы соответствовать конкретным физическим параметрам различных трубчатых ключей и используемой системы блокировки. В альтернативных вариантах эта область может быть размещена на губках ключа, или на его переднем конце, или рядом или в полый области внутри профилированного компонента 160, если таковая имеется. Рассмотренные выше проблемы и иллюстративные примеры касались цилиндрических и трубчатых ключей и замков, однако очевидно, что и другие типы ключей и замков могут быть без труда также адаптированы для использования в патентуемом способе и системе защиты универсальным ключом, предлагаемых в данном документе, так что дальнейшие примеры могли бы сочетать в себе указанные особенности, но не обязательно.

На фиг.8÷10 представлено несколько блок-схем, иллюстрирующих конкретные варианты осуществления, в том числе способа и системы защиты универсальным ключом согласно настоящему изобретению. Как показано на фиг.8, считывающая система 200 защиты универсальным ключом с несистемным управлением содержит по меньшей мере три базовых компонента - устройство 201 ввода/вывода ("ввод/вывод"), источник 202 питания и по меньшей мере один блок 203 памяти. В этой базовой системе устройство ввода/вывода может содержать, например, считыватель отпечатков пальцев, систему распознавания речи, устройство сканирования радужной оболочки глаза, цифровую наборную панель или любое другое подходящее устройство для считывания данных, ассоциированных с одним или более конкретными пользователями. Для такого устройства 201 ввода/вывода обычно требуется питание, которое поставляется посредством источника 202 питания, который может представлять собой, например, батарею, встроенную в рукоятку ключа, внешнюю батарею или источник питания переменного тока, подключенный через один или более контакты питания, или в некоторых случаях достаточный уровень высокочастотной энергии обеспечивается удаленным устройством высокочастотного питания и считывания. Устройство 201 ввода/вывода также обычно требуется обращение к одному или более хранимым управляющим файлам по меньшей мере в одном блоке 203 памяти для сравнения со специфическими входными данными пользователя при всякой попытке доступа. Такой блок памяти может представлять собой флэш-память, RAM или любые ЗУ самых различных типов, но предпочтительнее является какая-либо форма ROM или другого относительно стабильного ЗУ. Как было указано выше, этот считыватель с несистемным управлением обеспечивает считывание идентификационных признаков пользователя ключа и анализирует, а также аутентифицирует такие данные полностью внутри самого ключа, так что сигнал аутентификации посылается от самого ключа на замок

после подтверждения надлежащей информации о пользователе.

Как показано на фиг.9, альтернативная считывающая система 210 защиты универсальным ключом с системным управлением содержит не только устройство 211 ввода/вывода, источник 212 питания и по меньшей мере один блок 213 памяти, но и по меньшей мере три дополнительных базовых компонента. Ядро этой системы с системным управлением составляют ЦП 214, датчик с независимым управлением или другое устройство внутри электромеханического замка 215 и сеть 216. Как подробно описывается в случае предыдущей системы, устройство 211 ввода/вывода может представлять собой, например, считыватель отпечатков пальцев, систему распознавания речи, устройство сканирования радужной оболочки глаза, наборную клавишную панель или любое другое подходящее устройство для считывания данных, относящихся к одному или более конкретным пользователям. Такому устройству 211 ввода/вывода может требоваться питание, и такое питание может подаваться от батареи (не показанной), размещенной внутри самого устройства ввода/вывода, или, в другом варианте изобретения, от внешнего источника 212 питания непосредственно или через другой компонент типа ЦП 214. Имеется и по меньшей мере один блок 213 памяти для сравнения со специфическими входными данными пользователя при всякой попытке доступа, но в этом варианте с системным управлением обращение к такому блоку или блокам памяти обычно осуществляется со стороны ЦП 214 или, в альтернативном варианте изобретения, со стороны сети 216. Как и в вышеупомянутом случае, блок 213 памяти может представлять собой флэш-память, RAM или любые ЗУ самых различных типов, но предпочтительнее является какая-либо форма ROM или другого относительно стабильного ЗУ.

В варианте с системным управлением данные пересылаются из устройства 211 ввода/вывода 211, которое может быть, например, датчиком отпечатков пальцев или цифровой наборной панелью, в ЦП 214 и/или в сеть 216 для оценки и/или регистрации. ЦП 214, который может находиться внутри самого электромеханического замка, или в другом месте внутри игровой машины, или, в другом варианте изобретения, в некотором удаленном пункте, принимает данные из устройства 211 ввода/вывода и переходит к сравнению этих предлагаемых данных от активного пользователя с одним или более хранимыми файлами в одном или более блоках 213 памяти. Такой хранимый файл может содержать, например, множество признаков для конкретного отпечатка пальца авторизованного пользователя. В случае невозможности подтверждения совпадения никакой сигнал авторизации не посылается в электромеханический замок, так что замок не открывается. Если совпадение подтверждается, ЦП 214 может быть затем установлен в состояние автономной отправки сигнала авторизации, чтобы обеспечить возможность открывания замка, или перед этим может потребоваться подтверждение дополнительной информации из сети 216. Такая дополнительная информация может содержать данные о том, является ли данный пользователь в настоящее время все еще авторизованным в сети, или данный пользователь имеет ограничения по доступу к определенным машинам или по датам или времени доступа. Такая дополнительная информация из сети может запрашиваться ЦП перед, в процессе или после приема и анализа данных из устройства ввода/вывода, но для ЦП предпочтительнее не посылать сигнала авторизации в замок до получения положительной дополнительной информации из сети, позволяющей перейти к этой операции. Кроме того, для оказания системе помощи в деле принятия решения о разрешении открытия замка, сеть 216 в предпочтительном варианте также используется для постановки задач записи и

организации специфических фактических сведений, касающихся одного или более пользователей, машин и/или транзакций.

Если предположить, что содержимое одного или более файлов позволило достичь корректного совпадения данных активного пользователя и что из сети было получено
 5 подтверждение, если это было необходимо, то тогда ЦП 214 посылает сигнал авторизации в датчик с независимым управлением или другое устройство внутри электромеханического замка 215, обеспечивающий возможность последующего
 10 открытия замка, в предпочтительном варианте в течение времени, пока механический ключ остается в замке, чтобы повернуть замок физически во время открытия. Таким образом, ограничитель хода замка с электрическим управлением должен быть разблокирован по всему замку через отдельные механизмы или внутри защищенной
 15 среды или на расстоянии, что значительно затрудняет совершение жульнических или мошеннических действий по отношению к системе просто потому, что кто-то имеет механический ключ, адаптированный для физического вставления внутрь замка и манипулирования.

Фиг.10 иллюстрирует блок-схему конкретной сетевой инфраструктуры для создания способа и система защиты универсальным ключом согласно одному примеру
 20 осуществления настоящего изобретения. Сеть 300, которая может быть по существу подобна сети 216, рассмотренной выше, содержит ряд компонентов для эффективного использования патентуемых способов и систем защиты универсальным ключом, предлагаемых в данном документе, применительно к некоторому числу машин или
 25 даже ко всему заведению или сети заведений. Одна или более игровых машин 10 могут быть размещены во множестве точек или в банках, или автономными, или подключенными к сети с помощью любого требуемого рабочего средства подключения типа провода и общей шины 301, которая может быть подключена по меньшей мере к одному универсальному серверу 310.

В качестве такого универсального сервера 310 может быть использован уже
 30 имеющийся в заведении для одной или более других целей вместо или в дополнение к целям защиты. Другие функции для такого сетевого универсального сервера включают в себя, например, функции учета и начисления заработной платы, возможности Internet и электронной почты, коммутируемую связь, резервирование и
 35 другие гостиничные и ресторанные операции и другие различные операции для всего заведения. В отдельных случаях функции защиты могут быть также ассоциированы с таким универсальным сервером или выполняться таким универсальным сервером. Например, такой сервер может быть подключен к одной или более игровых машин
 40 внутри заведения и в некоторых случаях формировать сеть, которая включает в себя все или практически все машины внутри этого заведения. Средства связи могут при этом переключаться с каждой машины на одну или более программ, имеющих отношению к защите, на универсальном сервере. Например, сервер может быть
 45 запрограммирован на осуществление опроса каждой машины для всесторонней проверки защиты этой машины на регулярной основе. Кроме того, сервер может быть запрограммирован на осуществление текущего контроля за каждым потенциальным доступом в любой из игровых машин по месту ее нахождения, обеспечивающего
 50 возможность наблюдения и/или регистрации любой успешной или неуспешной попытки обращения к игровой машине с помощью устройств защиты универсальным ключом, предлагаемых в данном документе.

В особо предпочтительном варианте осуществления сеть 300 также содержит по меньшей мере один дополнительный специализированный сервер или сервер 320

защиты, который используется для различных функций, касающихся защиты, в сети защиты. Наличие такого дополнительного сервера защиты является желательным по множеству причин, типа снижения нагрузки на универсальный сервер или изоляции или отделения некоторой или всей информации о защите от универсального сервера и, таким образом, ограничения возможных режимов доступа к такой информации о защите. Кроме того, сервер 320 защиты может быть использован как исключительный управляющий модуль для удовлетворения любых требований сети в случае любых способов и систем защиты универсальным ключом, используемым заведением. В альтернативном варианте изобретения сеть 300 может быть изолирована от любой другой сети внутри заведения, так что универсальный сервер 310 будет совершенно бесполезным и будет использоваться специализированный сервер 320, выделенный исключительно для мероприятий по защите универсальным ключом. В вариантах осуществления как при изолированной сети, так и при сети с общей средой передачи данных сервер 320 защиты универсальным ключом в предпочтительном случае включает в себя подключения к сети 330 одного или более периферийных устройств, а также базы данных или другого подходящего носителя 340 данных. Среди периферийных устройств можно назвать один или более видеомониторов 331, один или более пользовательских терминала 332, один или более принтеров 333, одно или более других устройств 334 цифрового ввода типа считывателя карточек или другого идентификатора безопасности по желанию и не только.

База 340 данных в предпочтительном варианте адаптирована для хранения многих или всех файлов, относящихся к специфической пользовательской информации, так что к обращению к этим файлам может осуществляться непосредственно по запросу ЦП машины или в целях копирования. В этой базе данных может также храниться дополнительная информация относительно статуса и любых уместных ограничений относительно каждого прошлого или настоящего зарегистрированного пользователя. Кроме того, эта база данных может быть также адаптирована для хранения данных по транзакциям для каждого времени даже попыток доступа к игровой машине. Параметры для хранения таких элементов по транзакциям могут варьироваться в широких пределах и оставляются на усмотрение системных администраторов. Кроме того, база 340 данных в предпочтительном варианте непосредственно доступна для одного или более периферийных устройств в сети 330, подключенной к серверу 320 защиты универсальным ключом, так что данные, специфические для данных пользователей или транзакциям, зарегистрированные в базе данных, может быть без труда найдены и подвергнуты просмотру в одном или более периферийных устройствах. Кроме того, предполагается, что одно или более периферийных устройств в сети 330 может быть также подключено непосредственно к общей шине 301, как показано, хотя такая конструкция может быть нежелательной в зависимости от требуемого уровня защиты в сети 300.

На фиг.11 представлена типичная база данных, содержащая ассоциированные идентификаторы данных различных авторизованных и утративших авторизацию лиц согласно одному примеру осуществления настоящего изобретения. Подобно представленной на фиг.10 база 340 данных доступна для одного или более серверов, в предпочтительном варианте по меньшей мере серверу 320 защиты универсальным ключом 320, и имеет подключение к сети 330 одного или более периферийных устройств. База 340 данных в предпочтительном варианте содержит информацию по множеству предшествовавших транзакций доступа машин, а также информацию, касающуюся множества прошлых и настоящих авторизованных пользователей внутри

системы. Кроме того, база 340 данных может также содержать файлы относительно других лиц типа файлов биометрических данных известных мошенников или похитителей или подозреваемых, так чтобы возможно мошенническую попытку обращения к игровой машине можно было, в частности, без труда соотнести с известным неавторизованным лицом, не с кем-либо еще.

Содержимое базы 340 данных представляет собой многочисленные файлы относительно многих различных прошлых и настоящих пользователей системы, и в предпочтительном варианте все такие пользователи содержатся в базе 340 данных или в группе ассоциированных баз данных. Такие файлы могут быть классифицированы согласно файлам 341 авторизованных в настоящее время пользователей и файлам 342 прошлых, но утративших авторизацию пользователей. Содержимое каждого файла является профилем пользователя, имеющим многочисленные пункты информации, требования по ограничениям, если таковые вообще имеются, уровень или уровни доступа и, в предпочтительном варианте, по меньшей мере один файл аутентификации, содержащий информацию для того пользователя, который должен быть использован для аутентификации пользователя во время использования механического ключа. Как показано, для пользовательского файла 341А такая информация может включать в себя элементы типа, например, имя и номер сотрудника, дату начала, специфический номер для механического ключа или ключей, выданных этому сотруднику, информацию по ограничениям для этого сотрудника и один или более типов и файлов аутентификации файлов среди других. Информация по ограничениям может включать в себя казино, залы или помещения, доступ к которым этому сотруднику разрешен, типы машин, названия машин, номера машины, типы защиты, уровни доступа в каждой машине, ограничения по времени суток и датам, в которые машины доступны этим сотрудникам, и другую подобную информацию. Такая информация может не только храниться в пользовательском файле в базе данных, но может также быть найдена и использоваться сервером 320 защиты универсальным ключом и/или ЦП игровой машины, по отношению к которой предпринимается попытка доступа, чтобы определить, является ли пользователь с какой-либо другой авторизацией авторизованным для доступа по конкретному помещению, машине, уровню внутри машины, дате и времени суток, получить который он пытается.

Как было указано ранее, каждая защищенная среда с возможностью доступа по ключу, типа игровой машины, может иметь отдельные уровни защиты внутри машины, с отдельным статусом авторизации, требуемым для каждого уровня для каждого пользователя системы. Например, отдельная игровая машина может иметь различные уровни доступа для: I) своей главной дверцы, II) своего основного ЦП, III) своего банкнотоприемника и IV) своего монетоприемника. В этот список могут быть введены и дополнительные внутренние элементы, для которых может потребоваться введение дополнительных уровней защиты, по соображениям краткости и ясности в данном документе рассматриваются только четыре перечисленных уровня. Имеет ли пользователь доступ к одному из этих четырех уровней, в предпочтительном варианте не зависит от того, имеет ли этот же самый пользователь доступ к другому компоненту, если конечно при этом не требуется доступа к главной дверце или подобного более высокого уровня доступа для доступа с другой авторизацией к внутреннему компоненту, требующему открытия главной дверцы или более высокого уровня доступа.

В этом примере уровни доступа для конкретного пользователя могут определяться

как I-II-III-IV с "1" или "Y" в случае положительного ответа и "0" или "N" в случае отрицательного ответа в зависимости от того, действительно ли пользователь является авторизованным для каждого данного уровня. Например, механику Сэму предоставлены полномочия только на открытие главной дверцы игровой машины и
 5 никаких иных. Следовательно, пользовательский файл 341 для Сэма будет содержать обозначение "уровней доступа" 1-0-0-0. Точно также технику Джо разрешен доступ к главной дверце и к зоне ЦП игровой машины, так что обозначение уровня доступа для Джо будет читаться как 1-1-0-0. Далее, инкассатор Билл имеет обозначение уровня
 10 доступа 1-0-1-1, в то время как администратор Тэд - 1-1-1-1. Разумеется, могут добавляться уровни и обозначения уровней доступа для каждого пользователя, и эти обозначения могут меняться со временем или в некоторых случаях приобретать вид 0-0-0-0.

Когда зарегистрированный пользователь понижается в должности, увольняется или
 15 по другим причинам теряет некоторые или все привилегии доступа, ранее предоставленные этому пользователю, то файл такого пользователя может быть соответствующим образом обновлен системным администратором или, в другом варианте изобретения, повторно классифицирован как файл для пользователя,
 20 который больше не обладает никакими полномочиями. В таких случаях пользовательская информация и биометрические файлы могут храниться в базе данных, чтобы можно было использовать такую информацию в будущем при попытке несанкционированного доступа в какой-то момент. Кроме того, для некоторых систем использование таких входных данных с сервера защиты в сети, а не отдельных
 25 локальных файлов в отдельных ключах или машинах может быть критическим, так как обновлений статуса, касающихся потенциальных "деавторизаций", в таких локальных файлах может не происходить вообще или носить более случайный характер, чем в основной сети или на сервере. Был рассмотрен один пример базы
 30 данных для хранения файлов таких действительных пользователей или пользователей с запрещенной или отмененной авторизацией, которая может быть фирменной базой данных, спроектированной для специфических ассоциаций и использования в патентуемых способе и системе защиты ключом, рассматриваемых в данном документе, однако для этой же цели могут быть использованы и другие базы данных.
 35 Среди таких баз данных можно назвать, например, другие фирменные базы данных, ассоциированные с другими функциями в казино или заведении, частные базы данных других организаций, которые могут требовать или не требовать подписок для доступа и использования, и баз данных, находящихся в совместном использовании с
 40 правительственными организациями или регулирующими ведомствами.

Согласно одному примеру осуществления настоящего изобретения предлагаемые способ или система и, в предпочтительном варианте, сеть или подобная структура являются адаптированными для записи данных или информации, относящейся к
 45 попыткам доступа к игровой машине или устройству, предпринимаемым при совершении транзакции. Такой захват оперативных данных может использоваться немедленно в случае возникновения необходимости включения тревожной сигнализации, и эти данные могут также храниться неопределенно долго в одной или более базах данных типа базы данных, описанной выше. В случае необходимости
 50 включения одного или более устройств тревожной сигнализации при использовании настоящей системы защиты универсальным ключом предпочтительнее соединить ее с одним или более элементами системы и сети более высокого уровня в заведении или казино, такой что какое-либо касание клавиш, ошибочное нажатие кнопок на

наборной панели, неправильная ориентация или недостаточная экспозиция пальца или большого пальца руки на датчике отпечатков пальца или какая-либо другая человеческая ошибка автоматически не будет приводить к автоматическому включению устройства тревожной сигнализации и/или соответствующей ответной реакции.

Соединение с существующей системой защиты ключом может включать в себя использование, например, устройств тревожной сигнализации и одной или более камер системы безопасности и/или микрофонов, причем управление такими камерами и микрофонами может осуществляться из диспетчерской или зоны наблюдения, в результате чего первое устройство тревожной сигнализация просто сигнализирует оператору или автоматизированному компьютеру о необходимости сфокусировать по меньшей мере одну камеру на затронутой машине, чтобы осуществить текущий контроль и/или сделать запись потенциально проблематичной транзакции. Захват оперативных данных может использоваться и в других целях, многие из которых подразумевают хранение такой информации для последующего использования, например, в случае падения напряжения или отключения машины по другим причинам, для получения точного доказательства, подтверждающего версию оператора казино об имевшей место определенной транзакции, или отслеживания картины использования или злоупотребления по отношению к одной или более машинам или пользователям.

На фиг.12 представлена блок-схема, иллюстрирующая один способ создания способа и система защиты универсальным ключом согласно одному примеру осуществления настоящего изобретения. За этапом 370 начала следует первый этап 372 вставления ключа в замок, который инициирует процесс, после которого наступает последующий этап 374 подачи питания на механический ключ или включения этого ключа иным способом. В случае, когда биометрические или другие данные поступают из места, отличного от самого механического ключа, то на этапе 374 также происходит "включение" или инициирование такого поступления специфических пользовательских данных. На следующем этапе 376 происходит захват оперативных данных аутентификационной информации и возможно другой информации, относящейся к конкретной транзакции доступа. Оперативные данные, которые могут быть захвачены в дополнение к любым специфическим пользовательским хранимым файлам и имеющейся оперативной аутентифицирующей информации, могут включать в себя, например, информацию о специфической машине и ее местоположении, дату и время транзакции доступа, продолжительность доступа, различные уровни полученного доступа внутри машины, информацию о присутствии более чем одного авторизованного лица или около машины и др. Такой захват оперативных данных в предпочтительном варианте достигается через передачу данных, подвергаемых на практике шифрованию с помощью любых доступных программ или систем шифрования.

После сбора достаточного объема оперативных данных пользователя ключа, которые являются, например, данными отпечатка пальца, другими биометрическими данными или введенным ПИНом, происходит переход к этапу 378, на котором захваченные оперативные данные могут быть подвергнуты анализу. Анализ проводится на ЦП или другом подобном процессоре внутри ключа, замка, игровой машины или на удаленном процессоре в сети. После анализа захваченные или собранные оперативные данные подвергаются на этапе 380 сравнению с данными в управляющем файле, который хранится в одной или более ячеек памяти, как

описывалось более подробно выше. После выполнения такого сравнения инициируется запрос на наличие или отсутствие совпадения между захваченными оперативными данными и данными файла и происходит переход к этапу 382 принятия решения. При принятии решения о совпадении процесс продолжается на этапе 384, на котором замок открывается и разрешается доступ к машине или к внутреннему компоненту машины. На следующем этапе 386 в течение сеанса доступа или после его окончания результаты и данные направляются на сервер защиты универсальным ключом в сети, после чего сервер может принять решение об отказе от некоторых или всех результатов и данных или о сохранении некоторых или всех этих результатов и данных в ассоциированной базе данных, которое происходит на последующем этапе 388 регистрации результатов, после чего происходит переход к этапу 394 окончания процесса обработки данных. При любой передаче или обмене данными, результатами, командами или другой информацией в предпочтительном варианте данные подвергаются шифрованию с помощью любых доступных программ или систем шифрования.

Если же на этапе 382 принимается решение об отсутствии совпадения, то происходит переход к этапу 390, на котором обеспечивается запрет физического доступа ко всей игровой машине или к целевому внутреннему компоненту этой машины. Затем, на следующем этапе 392 инициируется последовательность сигналов тревоги, следствием которой может стать всеобщая тревога и инициирование ответного сигнала или уведомление другим сотрудникам и системам службы безопасности о необходимости уделения большего внимания затронутой игровой машине или устройству. После этапа 392 инициирования сигналов тревоги происходит воссоединение с основной ветвью процесса на этапе 386 пересылки информации, на котором сетевой сервер вновь может принять решение об отказе от некоторых или всех результатов и данных или о сохранении некоторых или всех этих результатов и данных в ассоциированной базе данных на последующем этапе 388 регистрации результатов, после чего происходит переход к этапу 394 окончания процесса обработки данных. Как и на предшествующих этапах процесса при любой передаче или обмене данными, результатами, командами или другой информацией в предпочтительном варианте данные подвергаются шифрованию с помощью любых доступных программ или систем шифрования.

В целях достижения ясности и понимания сути настоящее изобретение было выше описано на иллюстрациях и примерах. Однако следует осознавать, что в пределах существа или отличительных характеристик изобретения возможны многочисленные другие варианты и примеры его осуществления. В изобретение могут быть внесены определенные изменения и дополнения и очевидно, что оно не ограничивается рассмотренными частностями, а определяется объемом прилагаемой формулы изобретения.

Формула изобретения

1. Способ обеспечения безопасности в игровой машине, содержащий этапы: вставления механического ключа в электромеханический замок, охраняющий доступ к зоне с возможностью доступа по ключу внутри указанной игровой машины; считывания первого источника идентификационных признаков с указанного механического ключа, где указанный первый источник идентификационных признаков содержит информацию или данные, специфические для указанного замка; считывания второго источника идентификационных признаков, где указанный

второй источник идентификационных признаков содержит информацию, специфическую для одного или более пользователей указанного механического ключа; анализа указанного второго источника идентификационных признаков, относящегося к хранимому файлу с биометрической информацией в местонахождении,
5
отдельном от указанного механического ключа;

авторизации использования указанного механического ключа по результатам считывания указанных первых и вторых источников идентификационных признаков; ограничения доступа к указанной области с возможностью доступа по ключу по
10
выбору на основе одного или более дополнительных факторов и автоматического разрешения или отклонения доступа к указанной области с возможностью доступа по ключу в соответствии с решением на этапе авторизации.

2. Способ по п.1, отличающийся тем, что указанный первый источник
15
идентификационных признаков содержит одну или более физических характеристик указанного механического ключа.

3. Способ по п.2, отличающийся тем, что указанные одна или более физических характеристик указанного механического ключа содержат по меньшей мере один элемент, выбранный из группы, в состав которой входят физическая форма
20
указанного ключа, система бороздок указанного ключа и по меньшей мере часть краевого профиля указанного ключа.

4. Способ по п.1, отличающийся тем, что дополнительно включает в себя этап захвата оперативных данных, отражающих один или более параметров, ассоциированных с любым другим этапом.

5. Способ по п.1, отличающийся тем, что указанная биометрическая информация содержит информацию, относящуюся к отпечатку пальца.

6. Способ по п.1, отличающийся тем, что указанная биометрическая информация содержит по меньшей мере один элемент, выбранный из группы, в состав которой
30
входит информация по распознаванию лиц, распознаванию речи и сканированию сетчатки глаза.

7. Способ по п.1, отличающийся тем, что указанная информация, специфическая для одного или более пользователей указанного механического ключа, содержится в одном или более идентификаторах авторизованного пользователя.

8. Способ по п.7, отличающийся тем, что дополнительно включает в себя этап отмены предварительно зарегистрированного идентификатора пользователя.

9. Игровая машина, адаптированная для приема ставки, проведения игры на основе этой ставки и предоставления вознаграждения на основе результата игры,
40
содержащая:

по меньшей мере одну область с возможностью доступа по ключу, содержащую один или более внутренних компонентов игровой машины, адаптированных для использования в приеме ставки, проведении игры на основе этой ставки, предоставлении вознаграждения на основе результата игры или любой их
45
комбинации; и

электромеханический замок, защищающий указанную по меньшей мере одну область с возможностью доступа по ключу, причем указанный электромеханический замок адаптирован для автоматического разрешения или запрета доступа к указанной
50
области с возможностью доступа по ключу в зависимости от того, что авторизационный сигнал поставляется по результатам верификации механического ключа, имеющего корректный первый источник идентификационных признаков,

корректного второго источника идентификационных признаков, относящихся к пользователю указанного механического ключа, и

при этом доступ к вышеупомянутой области с доступом по ключу предоставляется или отклоняется по выбору на основе одного или более дополнительных факторов, где указанный второй источник идентификационных признаков содержит биометрическую информацию, относящуюся к указанному пользователю указанного механического ключа.

10. Игровая машина по п.9, отличающаяся тем, что указанный первый источник идентификационных признаков содержит по меньшей мере один элемент, выбранный из группы, в состав которой входят физическая форма указанного ключа, система бороздок указанного ключа и по меньшей мере часть краевого профиля указанного ключа.

11. Игровая машина по п.9, отличающаяся тем, что указанная биометрическая информация содержит информацию, относящуюся к отпечатку пальца.

12. Игровая машина по п.9, отличающаяся тем, что второй источник идентификационных признаков предусматривает использование аутентификации активного ПИНа.

13. Способ обеспечения защиты в игровой машине или ее компонентов, содержащий этапы:

вставления ключа в замок;

считывания источника идентификационных признаков пользователя, где указанный источник идентификационных признаков пользователя, содержит информацию, специфическую для одного или более пользователей указанного ключа;

анализа указанного второго источника идентификационных признаков, относящегося к хранимому файлу с биометрической информацией в местонахождении, отдельном от указанного ключа;

авторизации использования указанного ключа по результатам утвердительного считывания указанного источника идентификационных признаков пользователя;

ограничения доступа к указанной игровой машине или ее компонентам по выбору на основе одного или более дополнительных факторов и

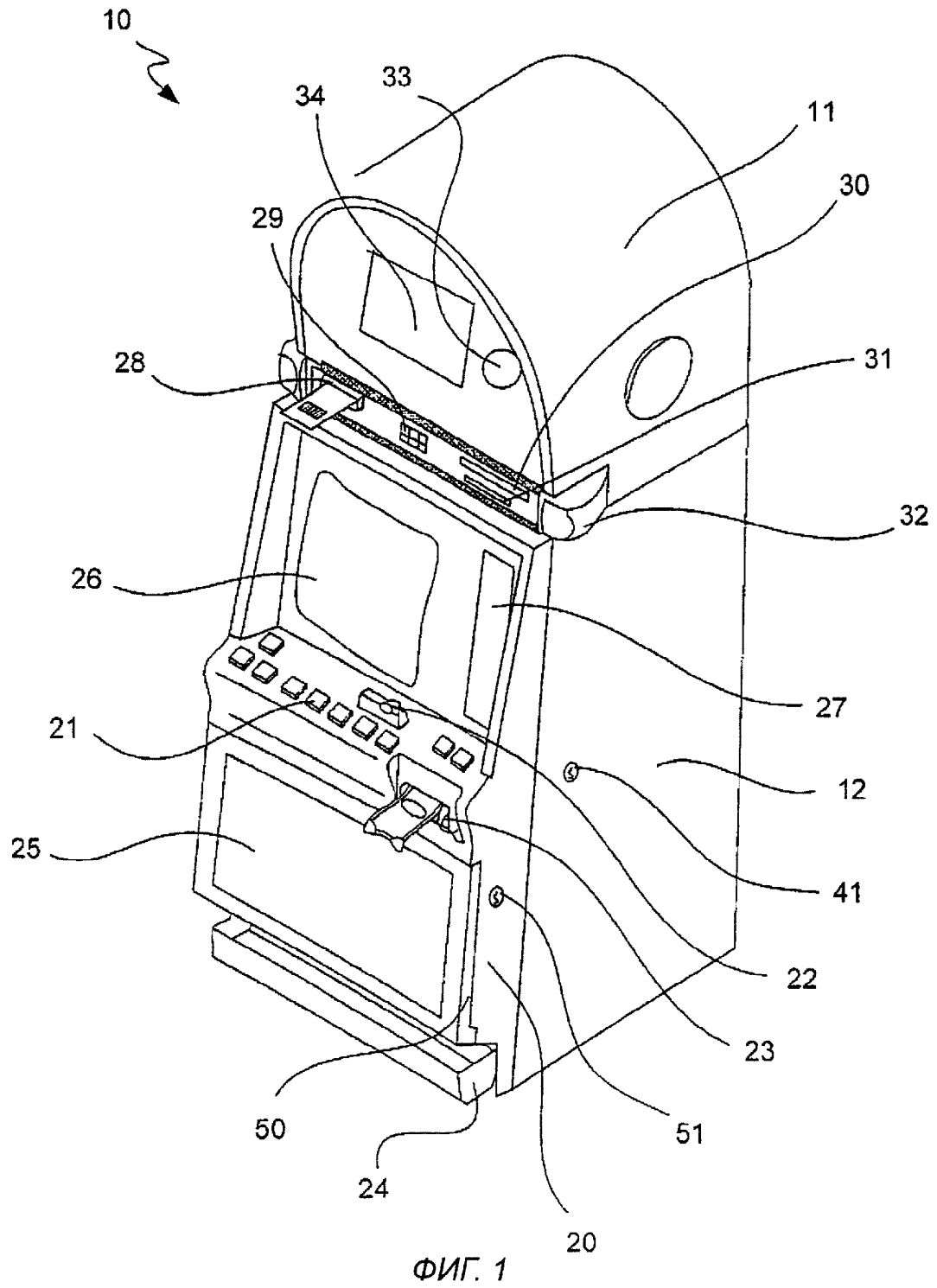
автоматического разрешения или отклонения доступа к указанной игровой машине или ее компоненту в случае, если данный ключ авторизован.

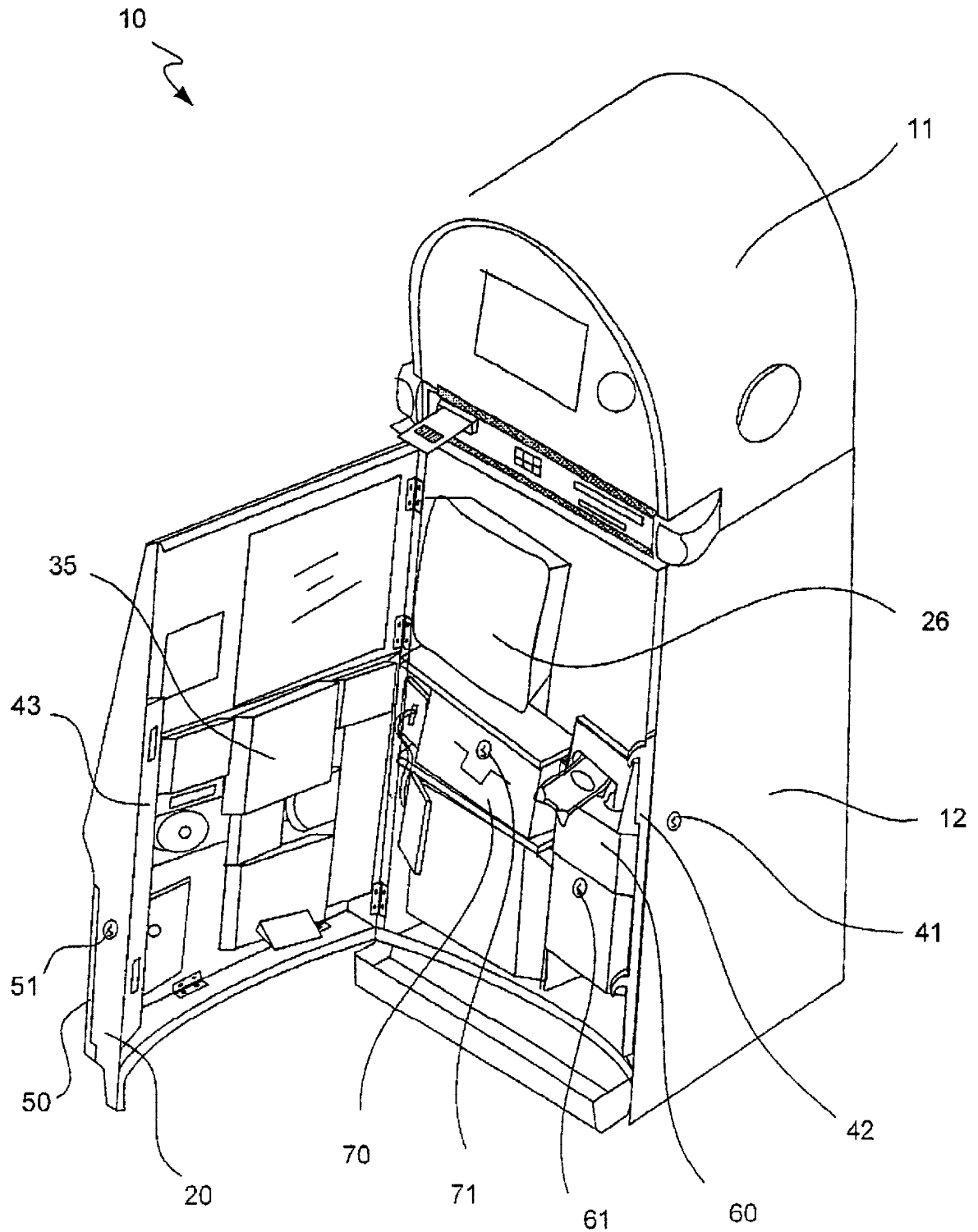
14. Способ по п.1 или 13, отличающийся тем, что один дополнительный фактор включает в себя использование заданных периодов времени.

15. Способ по п.13, отличающийся тем, что дополнительно включает в себя этап захвата оперативных данных, отражающих один или более параметров, ассоциированных с любым другим этапом.

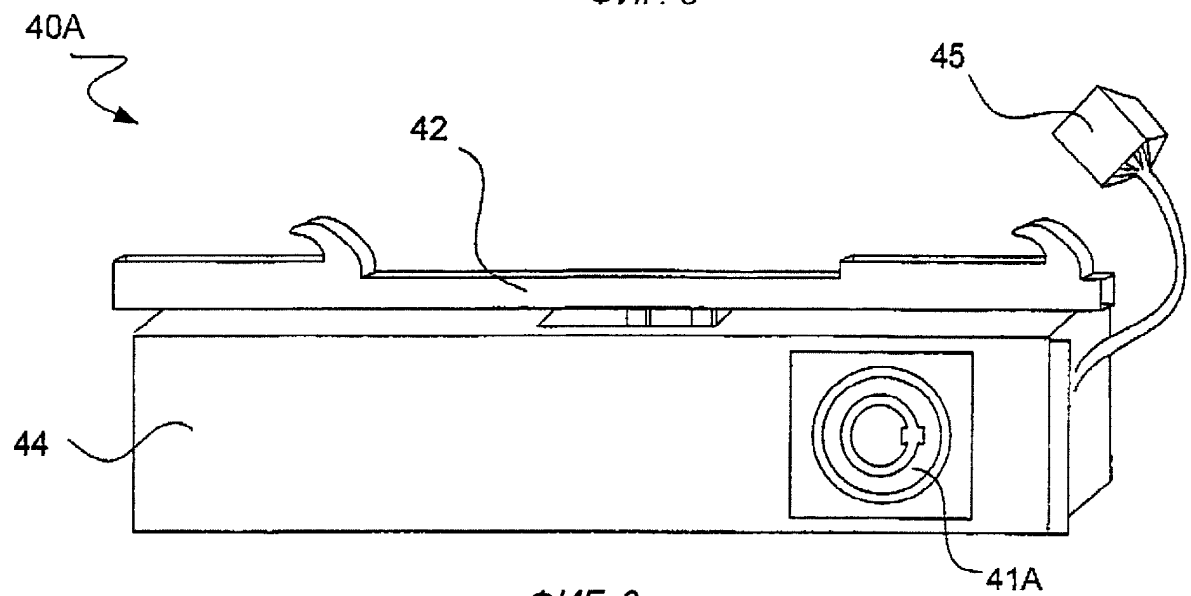
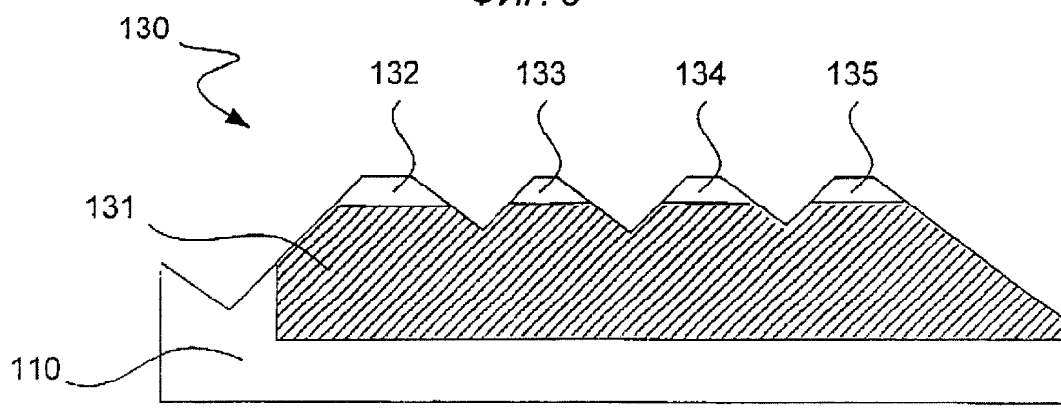
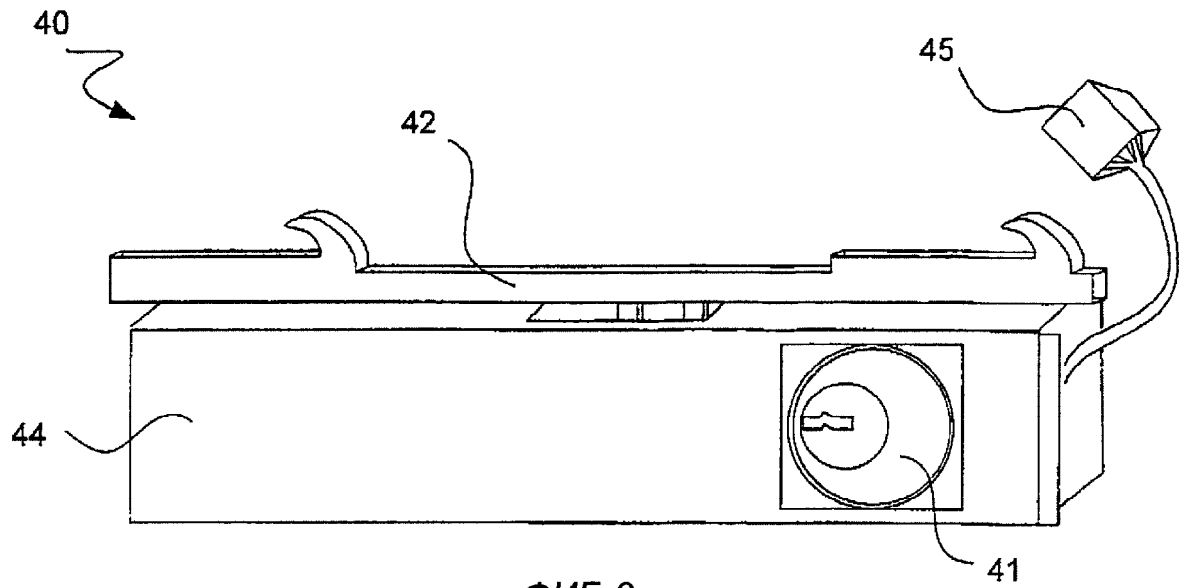
16. Способ по п.13, отличающийся тем, что указанная биометрическая информация содержит информацию, относящуюся к отпечатку пальца.

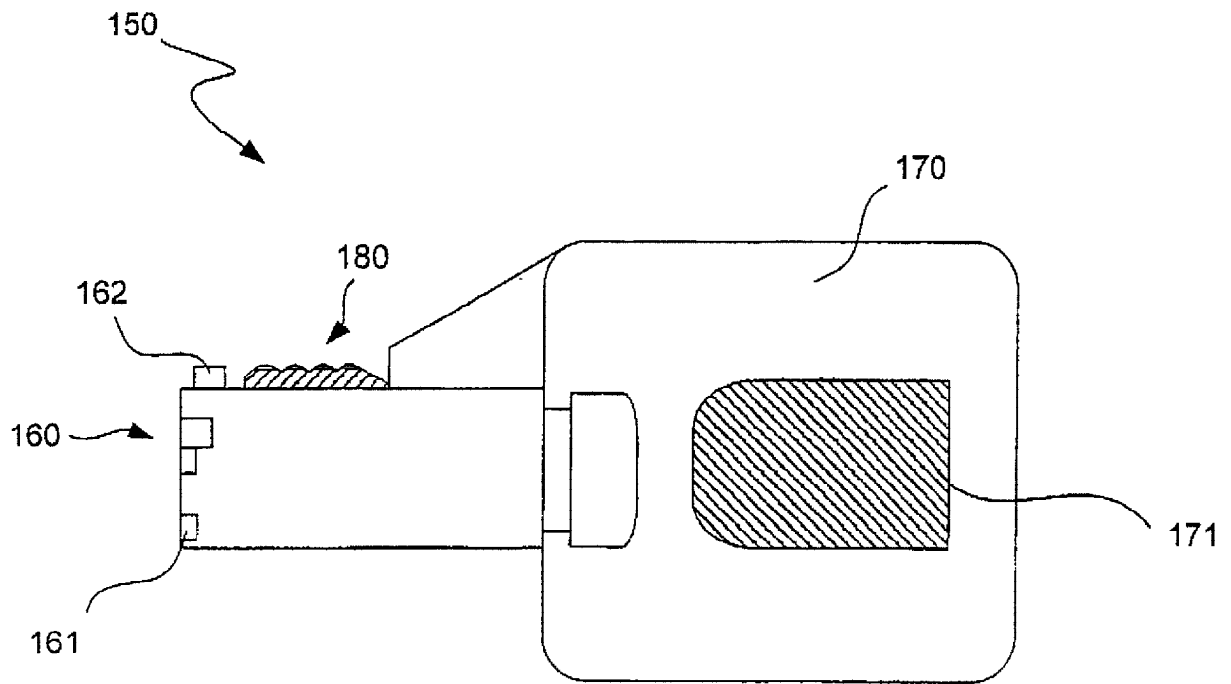
17. Способ по п.13, отличающийся тем, что указанная биометрическая информация содержит по меньшей мере один тип информации, выбранной из группы, в состав которой входит информация по отпечаткам пальцев, распознаванию лиц, распознаванию речи и/или сканированию сетчатки глаза.



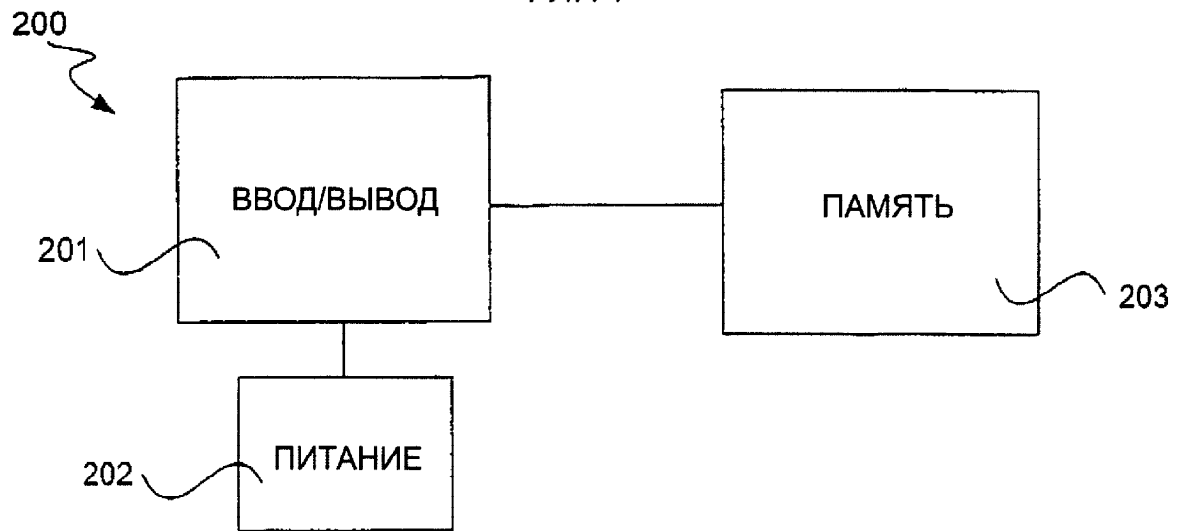


ФИГ. 2

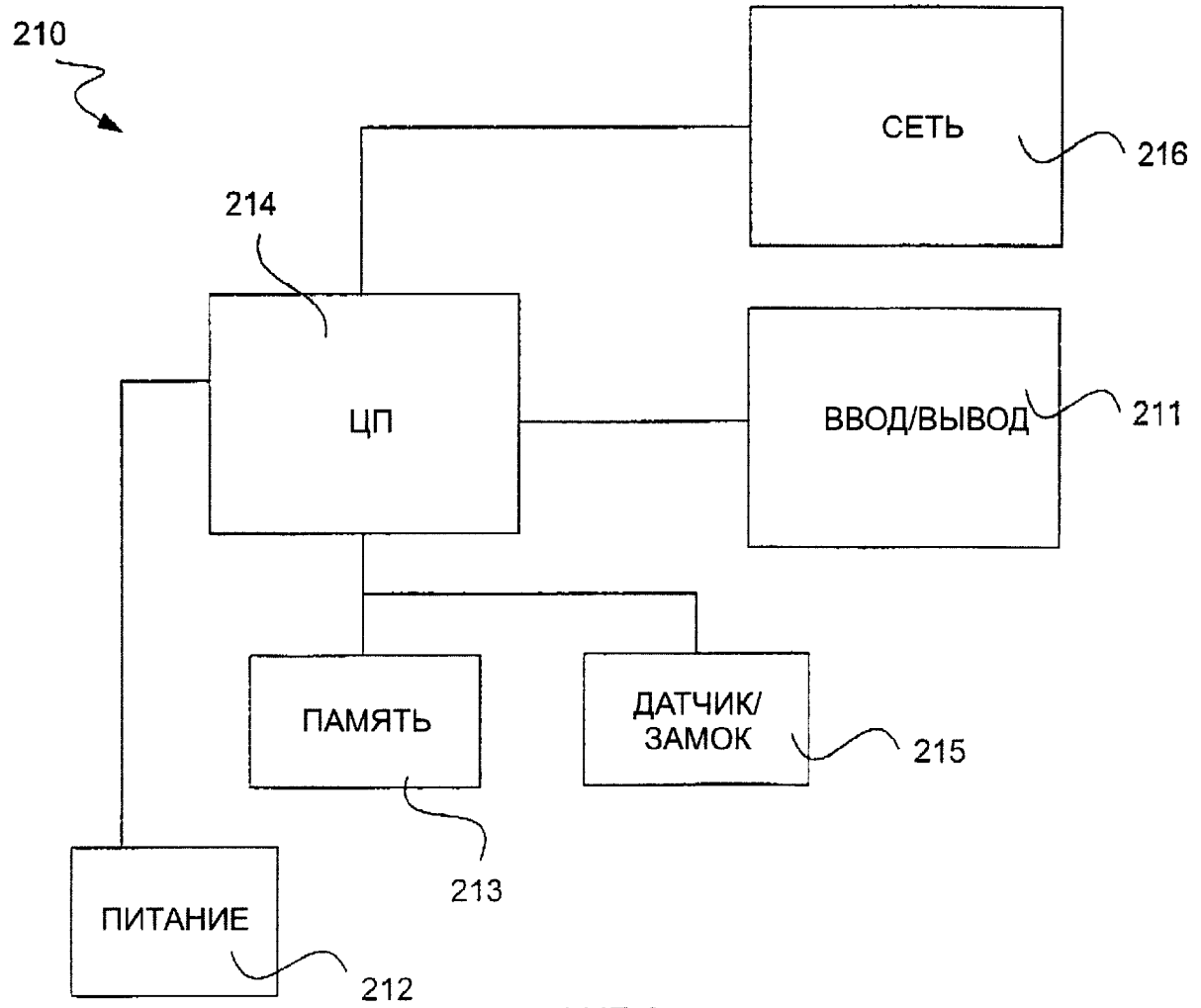




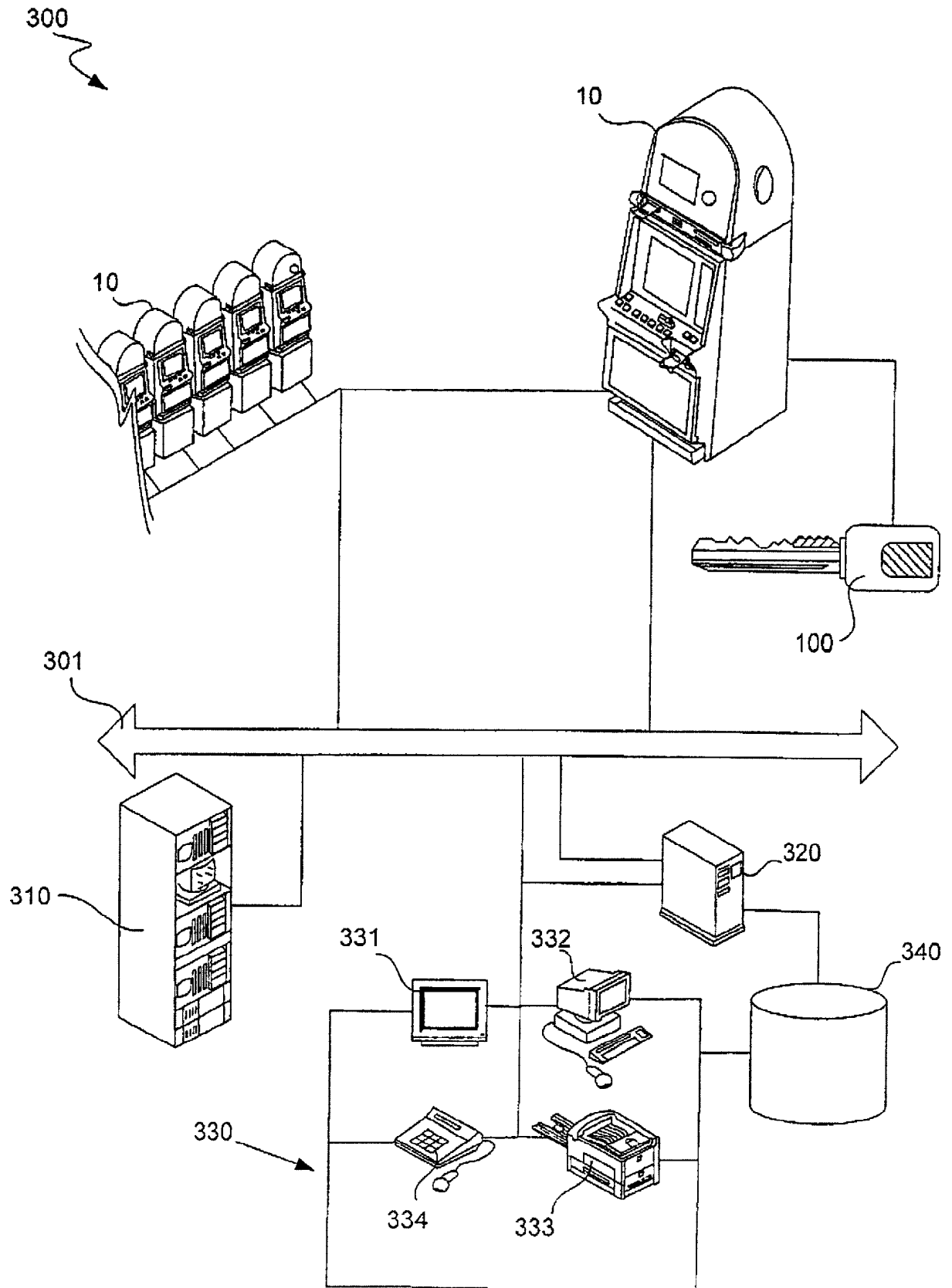
ФИГ. 7



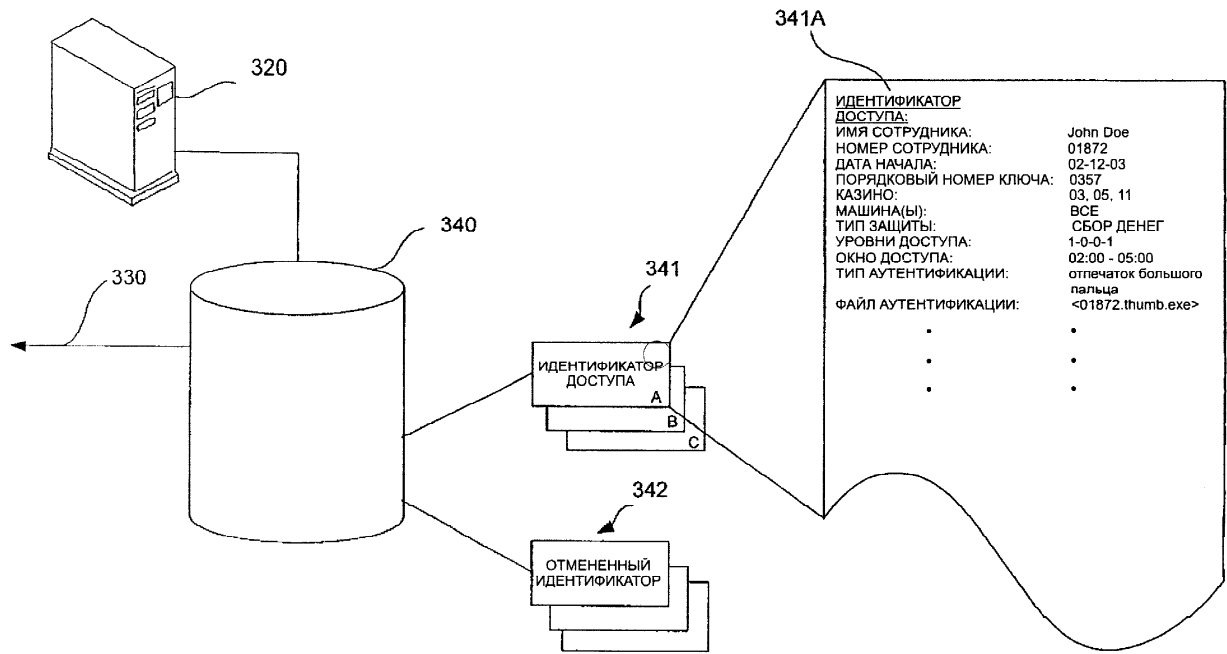
ФИГ. 8



ФИГ. 9



ФИГ. 10



ФИГ. 11

